REMARKS

Claims 1-20 are pending. Claims 1-20 were rejected under 35 U.S.C. § 103. Claims 1, 4, 5, 14-18 and 20 have been amended. Claim 21 has been added. Reconsideration and allowance of Claims 1-20, and allowance of Claim 21 is requested.

Rejection of Claims under 35 U.S.C. § 103

The Examiner rejected Claims 1-6, 9-14 and 17-20 under 35 U.S.C. § 103 as unpatentable over Chan et al. (U.S. Patent No. 6,005,942) in view of De Jong (U.S. Patent No. 5,802,519) and Le et al. (U.S. Patent No. 5,883,956).

Regarding Claim 1, the Examiner stated:

> Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). The operating system and security related code are stored in the ROM section (see column 1, line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing access permission data in the ROM section of the smart card. De Jong teaches a data structure for use in smart cards where access conditions (permissions) are stored in the memory means and are used to perform security measures (see column 8, lines 10-65 and column 12, lines 44-48). Neither Chan nor De Jong specifically teach the access permission data represents the availability of one or more cryptographic characteristics. Le teaches a secure processing unit embodied in a PersonCard (smart card) which uses a capability table that defines the cryptographic functions a secure processing unit can perform (see Abstract and column 7, line 50-et seq.) Le further shows the bit or bits within the capability table can specify the function or operating mode of a particular cryptographic operation, such as modulus size of the public-key pair or the allowable length of DES keys used by the particular function (see column 9, lines 19-58). It would have been obvious to one of ordinary skill in the art to combine the teachings of

Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see Le et al; column 2, lines 41-57].

As amended, Claim 1 recites (emphasis added):

> A cryptographic device, comprising:
> means for performing one or more cryptographic operations; and
> a data storage device or devices for storing access permission data representing the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein the data storage device or devices are adapted to enable all of the access permission data of the cryptographic device to be stored in the data storage device or devices after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

As indicated above, the Examiner stated that "Chan fails to specifically teach storing access permission data in the ROM section of the smart card" and that "[n]either Chan nor De Jong specifically teach the access permission data represents the availability of one or more cryptographic characteristics." Thus, as understood by Applicants, the Examiner has acknowledged that neither Chan et al. nor De Jong teach storing all of the access permission data of a cryptographic device (i.e., data representing the availability of one or more cryptographic characteristics) in data storage device(s) of the cryptographic device such that once value(s) of the access permission data are

stored in the data storage device(s), the value(s) of the access permission data cannot be changed. The Examiner further stated that "Le teaches a secure processing unit embodied in a PersonCard (smart card) which uses a capability table that defines the cryptographic functions a secure processing unit can perform" and that "[i]t would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications." However, the Examiner has not identified how Le et al. teach, alone or in combination with Chan et al. and/or De Jong, storing all of the access permission data of a cryptographic device in data storage device(s) of the cryptographic device such that once value(s) of the access permission data are stored in the data storage device(s), the value(s) of the access permission data cannot be changed. Thus, a prima facie case of unpatentability of Claim 1 has not been established.

Le et al. teach "[a] technique to dynamically configure a Secure Processing Unit (SPU) chip in a secure manner using a capability table, which defines the functions that an SPU can perform" (Abstract). Unlike the cryptographic device of Claim 1, in which all of the access permission data of the cryptographic device is stored in data storage device(s) of the cryptographic device such that once value(s) of the access permission data are

stored in the data storage device(s), the value(s) of the access permission data cannot be changed, in the invention taught by Le et al., a capability table stored for use by an SPU can be "overwritten" with a new capability table. For example, Le et al. teach at column 12, lines 10-23:

> [A]fter [a] digital signature has been verified, [a] function extracts [an] "enabling bit string" from [an] external capability table and stores it in non-volatile RAM inside the SPU. If there exists a current capability table in the SPU's non-volatile RAM, the value of the new capability table would simply overwrite the value of the current capability table. ... The "enabling bit string" that is loaded in the SPU becomes the new capability table which governs the functions that an SPU can perform.

In fact, the ability to overwrite a capability table stored for use by an SPU is believed by Le et al. to constitute a significant advantage of their invention as compared to previous SPUs. For example, Le et al. teach at column 3, lines 15-25:

> One approach which allows for customized configuration of an SPU depending upon the application with which it is used is through the use of different tables or vectors in Read-Only-Memory ("ROM") for different SPUs, which can enable or disable cryptographic functions. Under this approach, a manufacturer would program the ROM with firmware that implements a customer's specific security needs. A disadvantage with this method is that it does not offer the flexibility of allowing a system administrator to dynamically reconfigure an SPU once it has been installed in the field.

In contrast, Claim 1 recites that "[a] data storage device or devices are adapted to enable all of the access permission data of [a] cryptographic device to be stored in the data storage device or devices after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the data storage device or devices, the value or

values of the access permission data cannot be changed." A cryptographic device as recited in Claim 1 has advantageous characteristics as compared to the SPUs described by Le et al. For example, Applicants' specification states at page 10, line 10 to page 11, line 3:

> Preferably, the access permission data of the cryptographic characteristic table 403 are stored in a programmable read-only memory (PROM). The use of such a data storage device enables flexibility in establishing the access permission data (i.e., the availability of cryptographic characteristics) of a cryptographic device, since the access permission data can be established at device fulfillment (see FIG. 1). Thus, a single mass-produced type of cryptographic device can be tailored to meet cryptographic needs for many different applications. Further, the use of such a data storage device enables permanency - and, therefore, security - in establishing the access permission data of a cryptographic device, since once the access permission data are established, the access permission data cannot be changed. Thus, a single mass-produced type of cryptographic device can be tailored to satisfy domestic demand for robust cryptographic capabilities or to conform to export regulations dictating somewhat less robust cryptographic capabilities, while, in the latter case, providing confidence that the limitations on the cryptographic capabilities cannot be circumvented once the cryptographic device has been exported to a user.

Le et al. do not teach, either alone or in any combination with the teaching of Chan et al. or De Jong, a cryptographic device as recited in Claim 1, having the above-decribed advantageous characteristics. Thus, Claim 1 is allowable over the combination of Chan et al., De Jong and Le et al.

Claims 2 and 3 each depend on Claim 1 and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 1.

As amended, Claim 4 recites (emphasis added):

> A computer readable storage medium or media of a cryptographic device, the computer readable storage medium or media encoded with instructions and/or data, comprising:
>
> instructions and/or data for performing one or more cryptographic operations; and
>
> access permission data stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more cryptographic operations are performed by the cryptographic device, wherein all of the access permission data is stored in a storage medium or media after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the storage medium or media, the value or values of the access permission data cannot be changed.

As discussed above with respect to Claim 1, Chan et al., De Jong and Le et al. do not teach, either alone or in any combination, a computer readable storage medium or media of a cryptographic device in which "access permission data is stored in a storage medium or media after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the storage medium or media, the value or values of the access permission data cannot be changed," as recited in Claim 4. Thus, Claim 4 is allowable over the combination of Chan et al., De Jong and Le et al.

Claims 5 and 18 each depend on Claim 4 and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 4.

Regarding Claim 6, the Examiner stated:

Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1, line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). It would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see Le et al; column 2, lines 41-57].

Claim 6 recites (emphasis added):

> A cryptographic device, comprising:
>
> a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;
>
> one or more data storage devices for storing <u>a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation</u>, and a second set of instructions and/or data, distinct from the first set of instructions

and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

As indicated above, the Examiner stated that "[n]either Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device." The Examiner further stated that "Le teaches an external bus interface between [a] secure processing unit and a host system" and that "[t]his bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (column 7, lines 17-21)," then concluded that "[i]t would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications." Even assuming arguendo that the foregoing characterization of the teaching of Le et al. and its relationship to the teaching of Chan et al. and De Jong is true, such teaching is inapposite with respect to Claim 6, since Claim 6 recites "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "allowing access to the first set of instructions and/or data

from a device external to the cryptographic device." It has not been contended that Chan et al., De Jong or Le et al. teach or suggest a cryptographic device having such characteristics, alone or in any combination. Thus, a prima facie case of unpatentability of Claim 6 has not been established and Claim 6 is allowable over the combination of Chan et al., De Jong and Le et al.

A cryptographic device as in Claim 6 provides advantageous characteristics relative to previous cryptographic devices. For example, the first set of instructions and/or data recited in Claim 6 can be instructions and/or data for performing mathematical primitive operations (see, e.g., page 11, line 23 to page 12, line 6 of Applicants' specification). As stated in Applicants' specification at page 12, lines 6-19:

> .... Exposing the mathematical primitive operations to the applications developer provides flexibility to the applications developer in creating application code.
>
> For example, to add a new cryptographic operation or modify an existing cryptographic operation, it is not necessary to download to the cryptographic device all of the code necessary to accomplish the cryptographic operation. Rather, since the mathematical primitive operations are already accessible on the cryptographic device 400, the applications developer can provide code at a higher (and simpler) level of abstraction that includes instructions, as necessary, to effect performance of the required mathematical primitive operations.

Claims 9-13 each depend on Claim 6, either directly or indirectly, and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 6.

Claim 14 recites (emphasis added):

> A computer readable storage medium or media encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:
>
> a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation;
>
> a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and
>
> a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part.

It has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a computer readable storage medium or media encoded with one or more computer programs including "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part," as recited in Claim 14. Thus, a prima facie case of unpatentability of Claim 14 has not been established and Claim 14 is allowable over the combination of Chan et al., De Jong and Le et al.

Claim 17 depends on Claim 14 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 14.

Claim 19 depends on Claim 6 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 6.

Claim 20 depends on Claim 14 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 14.

The Examiner rejected Claims 7, 8, 15 and 16 under 35 U.S.C. § 103 as unpatentable over Chan et al. (U.S. Patent No. 6,005,942) in view of De Jong (U.S. Patent No. 5,802,519), Le et al. (U.S. Patent No. 5,883,956) and Ehrsam et al. (U.S. Patent No. 3,962,539).

Regarding Claim 7, the Examiner stated:

> Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1, line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device nor do either teach the sub-operations are comprised of one or more mathematical primitive operations. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). Ehrsam teaches a device for ciphering a block of data using a

> cipher key wherein the mathematical primitive operation includes a divide operation (see column 11, line 36-et seq.) and an XOR operation (see column 20, lines 15-17 and Figures 3a, 3b, 3c, 3d, 3e, 3f, 3g, 3h, 3i, 3j and 8). It would have been obvious to one of ordinary skill in the art to combine the teachings of Ehrsam's product block cipher system for data security, Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card in order to provide the cryptographic designer with the details of how the key bits within the particular permutation are to be used for generating the keys for the specific cryptographic operation [see Ehrsam et al.; column 2, line 32 to column, 4, line 51].

Claim 7 depends on Claim 6 and so includes the limitations of that claim. As discussed above, it has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a cryptographic device including "one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device," as recited in Claim 6. Nor has it been contended that Ehrsam et al. teach or suggest, alone or in any combination with the teaching of Chan et al., De Jong or Le et al., a cryptographic device having such characteristics. Thus, a prima facie case of unpatentability of Claim 7 has not been established and Claim 7 is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al.

Claim 8 depends on Claim 7 and so is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al. for at least the reasons given above with respect to Claim 7.

Claim 15 depends on Claim 14 and so includes the limitations of that claim. As discussed above, it has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a computer readable storage medium or media encoded with one or more computer programs including "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part," as recited in Claim 14. Nor has it been contended that Ehrsam et al. teach or suggest, alone or in any combination with the teaching of Chan et al., De Jong or Le et al., a computer readable storage medium or media encoded with one or more computer programs including such instructions. Thus, a prima facie case of unpatentability of Claim 15 has not been established and Claim 15 is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al.

Claim 16 depends on Claim 15 and so is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al. for at least the reasons given above with respect to Claim 15.

In view of the foregoing, it is requested that the rejection of Claims 1-20 under 35 U.S.C. § 103 be withdrawn.

New Claim

Claim 21 has been added. Support for Claim 21 can be found in Applicants' specification at, for example, page 11, line 23 to page 12, line 19.

Claim 21 recites (emphasis added):

> A cryptographic device, comprising:
> a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;
> one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and
> means for allowing a third set of instructions and/or data that is distinct from both the first and second sets of instructions and/or data, and that is used to perform one or more cryptographic operations to, after manufacture of the cryptographic device, be stored on the one or more data storage devices, and/or cause performance of instructions and/or access of data from the first set of instructions from a device external to the cryptographic device.

A cryptographic device as recited in Claim 21 does not appear to be taught or suggested by the above-discussed references cited by the Examiner in the instant Office Action. Such a cryptographic device has advantages over previous cryptographic devices as discussed above with respect to Claim 6.

CONCLUSION

Claims 1-20 were pending and were rejected. Claims 1, 4, 5, 14-18 and 20 have been amended. Claim 21 has been added. In view of the foregoing, it is requested that Claims 1-21 be allowed. If the Examiner wishes to discuss any aspect of this application, the Examiner is invited to telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on April 5, 2004.

4-5-04 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants